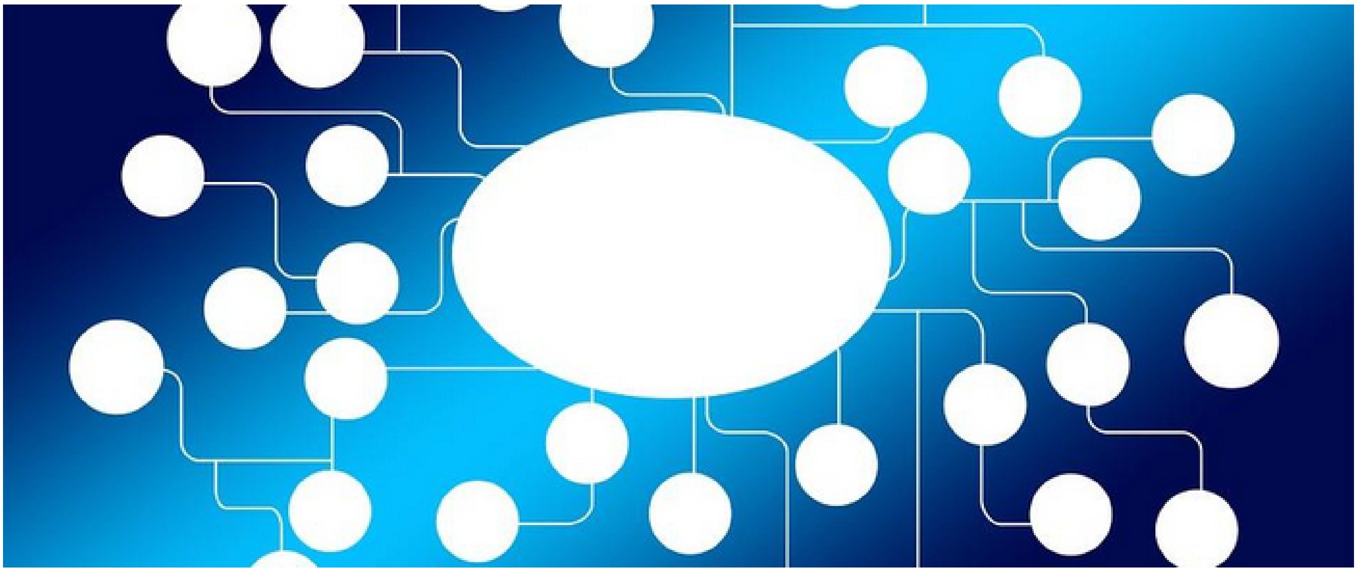

Effective national security requires anticipating threats and threat environments. It is not enough to work to solve today's information sharing challenges. Part of the Office of the Program Manager for the Information Sharing Environment's (PM-ISE) role in accelerating information sharing is imagining what information sharing will look like -- and what sharing challenges the world will face -- in the future. The threat picture is constantly evolving, and so must our information sharing policies, techniques, and technology into a collaborative strategy that will meet the security challenges of tomorrow.

The purpose of Project Interoperability (PI), a collaboration between the Standards Coordinating Council (SCC) and PM-ISE, is to promote the development of Information Sharing Environments (ISEs) between federal, state, local, tribal, and private sector mission partners at the domestic nexus of national security and public safety. Further, PI advocates for particular standards and technologies most likely to achieve the desired information sharing results and future compatibility between those ISEs.

Interoperability is the ability to transfer and use information in a consistent, efficient way across multiple organizations and IT systems to accomplish operational missions. From a technical point of view, interoperability is developed through the consistent application of design principles and standards to address a specific mission problem. Administrative preconditions to interoperability, such as policies and procedures, must be in place to exchange and safeguard the information.

Building on the foundation of both legislative and executive intent, the ISE strategy will require new frameworks and policies for implementation. Policy innovations and technical tools have helped accomplish many of the key goals and objectives of the National Strategy for Information Sharing and Safeguarding (NSISS). PM-ISE has government-wide authority to plan, oversee the build-out, and manage use of the ISE originally tasked in Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA). Additionally, PM-ISE is responsible for providing oversight of the Strategic Implementation Plan for the 2012 NSISS.

Existing authorizations, mission focus, and foundations are the point of departure for building the next generation of the ISE. PI achieves its mission through an integrated suite of technical and operational resources and expertise facilitating the planning, development, and optimization of ISEs to share terrorism-related information and other mission-critical information. Those resources include the ISE Core Interoperability Framework (ICIF) and the ISE Integration Library.

Information Sharing and Safeguarding Core Interoperability Framework (ICIF)

ICIF, a critical component of PI, is an assertion-based architecture to facilitate interoperable trust at machine speed. An assertion is a rigorously defined, machine-readable statement of compliance with a specific set of technical or business requirements. More than a decade of work on the information challenges faced by the nation has yielded several key foundational frameworks and products. Together, they have set the path for government-wide information sharing to enable a number of critical national security and public safety missions. Under the umbrella of Project Interoperability, PM-ISE has partnered with the Standards Coordinating Council (SCC), the IJIS Institute, and others to develop an Information Sharing and Safeguarding Core Interoperability Framework (ICIF) that will enable identity and security credentials (“assertions”) to be exchanged and independently vetted at machine speed. This capability will, in turn, exponentially reduce the time and effort it takes to conclude information sharing agreements (ISAs) between organizations, permitting ISEs to be rapidly established and expanded in time of need.

The ICIF is designed for those committed to building an ISE(s) to effectively share terrorism-related information. The ICIF Project, which is expected to produce a working prototype in 2017, uses the principles of service-oriented architecture such as reuse and intrinsic interoperability to identify standards, capabilities, and methodologies that can be used to link systems and establish, extend, or upgrade ISEs. Stakeholders include such federal counterterrorism ISE participants as the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the Intelligence Community (IC), as well as various regional and statewide information sharing environments that are intended to be compatible with the federal terrorism-related ISE, now or in the future.

The ICIF is the product of years spent in advancing the information sharing mission across federal, state, local, tribal, and private partner spaces. Once published, the ICIF will allow partners to independently build linkages and scale ISE-based solutions to ensure the right people have the right information at the right time.

The ISE Integration Library consists of various resources including an Information Sharing and Safeguarding Playbook to help with ISE implementations, common lexicon, training, policies, governance, and more. PI is designed for executives, managers, and implementers committed to building and sustaining an ISE.

As data relevant to counterterrorism and public safety becomes available in quantity and IT systems begin to expand, the importance of information interoperability will continue to grow. Projects like ICIF will enhance efforts to create a fully-integrated ISE to support the demands of federal, state, local, and tribal partners in the efforts to combat counterterrorism. PM-ISE will continue to sponsor and promote key foundational frameworks and products to set the path for government-wide information sharing to enable a number of critical national security and public safety missions.